

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-134193

(43)Date of publication of application : 12.05.2000

(51)Int. CI.

H04L 9/08

G06F 13/00

(21)Application number : 10-308007

(71)Applicant : FUJITSU LTD

(22)Date of filing : 29.10.1998

(72)Inventor : MATSUMOTO TATSURO  
MATSUI KAZUKI

## (54) SECURITY BUILDUP METHOD AND SYSTEM

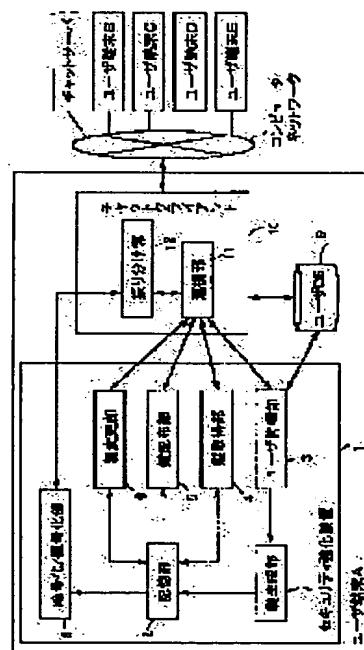
## (57)Abstract:

PROBLEM TO BE SOLVED: To prevent a common encryption key from being decoded and to facilitate its management.

SOLUTION: This system is provided with a storage section 2, an encryption/ decoding section 8, a user management section 3, a key acquisition section 4, and a key distribution section 5.

When the user management section 3 takes part in any channel, the section 3 acquires user information including a nickname list from a chat client and stores it. The key acquisition section 4 selects any user terminal to request an encryption key and stores the encryption key that is sent on request to the storage section 2. Upon the request from other user terminal, the key distribution section 5 distributes the encryption key read from the storage section 2 to the other user terminal. Furthermore, the

system is also provided with a key revision section 6 to preferably prevent the key from being decoded by revising the encryption key under a prescribed trigger. It can also be thought that key distribution attribute and key revision attribute are added to user information, and the encryption key is distributed or updated based on the sets of the attribute.



## LEGAL STATUS

[Date of request for examination]

29.10.2001

[Date of sending the examiner's  
decision of rejection]

[Kind of final disposal of application  
other than the examiner's decision of  
rejection or application converted  
registration]

[Date of final disposal for  
application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's  
decision of rejection]

[Date of requesting appeal against  
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998, 2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-134193

(P2000-134193A)

(43) 公開日 平成12年5月12日 (2000.5.12)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 C 5 B 0 8 9
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 J 1 0 4
		H 0 4 L 9/00	6 0 1 E
			6 0 1 A

審査請求 未請求 請求項の数23 O L (全 16 頁)

(21) 出願番号 特願平10-308007

(22) 出願日 平成10年10月29日 (1998. 10. 29)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番1号

(72) 発明者 松本 達郎

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

(72) 発明者 松井 一樹

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

(74) 代理人 100094145

弁理士 小野 由己男 (外2名)

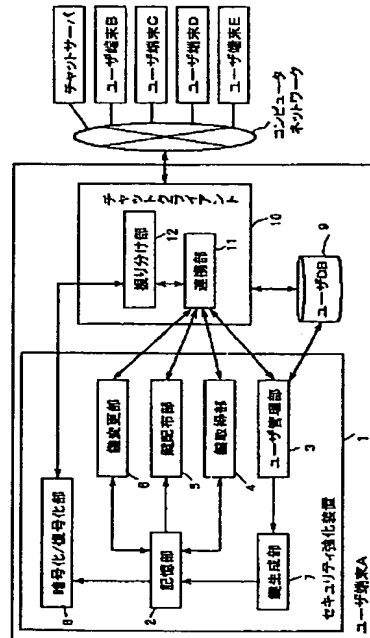
最終頁に続く

(54) 【発明の名称】 セキュリティ強化方法及び装置

(57) 【要約】

【課題】 共通の暗号鍵の解読を防止し、且つ管理を容易にする。

【解決手段】 記憶部2、暗号化／復号化部8、ユーザ管理部3、鍵取得部4及び鍵配布部5を備える。ユーザ管理部3は、いずれかのチャネルに参加した場合、ニックネームリストを含むユーザ情報をチャットクライアントから取得し、格納する。鍵取得部4は、いずれかのユーザ端末を選択して暗号鍵を要求し、要求に応じて送信される暗号鍵を記憶部2に格納する。鍵配布部5は、他のユーザ端末から暗号鍵の要求があった場合、記憶部2から読み出した暗号鍵を他のユーザ端末に配布する。また、さらに鍵変更部6を設けて一定のトリガで暗号鍵を変更し、鍵の解読を防ぐことが好ましい。鍵配布属性や鍵変更属性をユーザ情報に付加して設定し、これら属性に基づいて暗号鍵の配布や更新を行うことも考えられる。



## 【特許請求の範囲】

【請求項 1】互いに同一のネットワークを共有して同時に双方向通信が可能な通信装置に用いられ、前記ネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を、前記通信装置上で生成し、前記通信装置を用いてネットワークに参加した後に、前記ネットワークを共有するいずれかの他の通信装置に対して前記暗号鍵を要求し、前記ネットワーク内の他の通信装置からの暗号鍵の要求に応じ、前記準備した暗号鍵を要求元の通信装置に付与し、前記ネットワーク内の通信装置間の通信内容を、前記暗号鍵を用いて暗号化及び復号化する、セキュリティ強化方法。

【請求項 2】他の通信装置と互いに同一のネットワークを共有して同時に双方向通信が可能な通信装置とともに用いられ、前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を保持する記憶手段と、通信内容を前記通信装置から取得し、前記暗号鍵を用いて暗号化する暗号化手段と、通信内容を前記通信装置から取得し、前記暗号鍵を用いて復号化する復号化手段と、前記通信装置が前記いずれかのネットワークに参加している場合に、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を前記通信装置から取得し、前記記憶手段に格納する利用者管理手段と、前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する鍵取得手段と、他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布可能な鍵配布手段と、を備えるセキュリティ強化装置。

【請求項 3】前記通信装置は、前記セキュリティ強化装置との連携手段を有し、前記連携手段は、前記暗号鍵の要求、前記要求に応じて送信される暗号鍵、前記利用者情報に関する情報及び所定の条件に合致する場合は通信内容の受け渡しを、前記通信装置とセキュリティ強化装置との間で行う、請求項 2 に記載のセキュリティ強化装置。

【請求項 4】前記利用者管理手段は、他のセキュリティ強化装置に暗号鍵の配布を許可する鍵配布属性を、前記取得した利用者情報に基づいて設定し、前記記憶手段に格納する、請求項 2 に記載のセキュリティ強化装置。

【請求項 5】前記利用者管理手段は、所定の条件に基づいて、他の通信装置を選択し、前記暗号鍵の配布を許可する鍵配布属性を前記他の通信装置に付与し、かつ鍵配

布属性の設定及び設定対象の通信装置を前記通信装置から取得し、前記記憶手段に格納する、請求項 2 に記載のセキュリティ強化装置。

【請求項 6】前記利用者管理手段は、他の通信装置の選択と、前記暗号鍵の配布を許可する鍵配布属性の前記他の通信装置への付与及び解除の指示とを受け付け、かつ鍵配布属性の設定及び設定対象の通信装置を前記通信装置から取得し、前記記憶手段に格納する、請求項 2 に記載のセキュリティ強化装置。

【請求項 7】前記鍵取得手段は、所定の条件に基づいて前記暗号鍵の要求先を選択する、請求項 2 に記載のセキュリティ強化装置。

【請求項 8】前記鍵取得手段は、所定の条件に基づいて前記暗号鍵の要求先を選択して前記暗号鍵を要求し、所定時間内に前記要求先から暗号鍵が送信されない場合、他の通信装置を選択して再度要求を行う、請求項 2 に記載のセキュリティ強化装置。

【請求項 9】前記鍵取得手段は、前記通信内容が暗号化されている場合に前記暗号鍵の取得要求を行う、請求項 2 に記載のセキュリティ強化装置。

【請求項 10】前記復号化手段は、前記通信装置から受け取る通信内容を復号不可能と判断した場合、前記暗号鍵の要求を行うことを決定し、前記鍵取得手段は、前記復号化手段の決定に従い、前記暗号鍵の取得要求を行う、請求項 2 に記載のセキュリティ強化装置。

【請求項 11】前記記憶手段は、複数の暗号鍵と暗号鍵を特定する鍵識別情報とを対応付けて記憶し、前記暗号化手段は、前記通信内容の暗号化に用いられた暗号鍵を示す鍵識別情報と通信内容とを、前記通信装置を介してネットワークに送出可能であり、前記復号化手段は、前記鍵識別情報で特定される暗号鍵が前記記憶手段に保持されているか否かを判断し、前記鍵取得手段は、前記判断結果に従い、前記鍵識別情報を通知して前記暗号鍵の取得要求を行う、請求項 2 に記載のセキュリティ強化装置。

【請求項 12】前記鍵取得手段は、利用者の公開鍵暗号系の公開鍵を前記暗号鍵の要求とともに通知し、前記要求に応じて送信される暗号鍵を利用者の秘密鍵を用いて復号化し、

前記鍵配布手段は、前記要求元の公開鍵暗号系の公開鍵を用いて暗号化した前記暗号鍵を配布する、請求項 2 に記載のセキュリティ強化装置。

【請求項 13】前記鍵配布手段は、他の前記通信装置から前記暗号鍵の要求があった場合、前記要求を検証し、検証結果に基づいて前記記憶手段からいずれかの暗号鍵を読み出し、前記他の通信端末に配布可能である、請求項 2 に記載のセキュリティ強化装置。

【請求項 14】所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備え

る、請求項2に記載のセキュリティ強化装置。

【請求項15】所定のタイミングで前記暗号鍵を更新し、前記更新した暗号鍵を直前の暗号鍵を用いて暗号化して他の通信装置に配布する鍵変更手段をさらに備える、請求項2に記載のセキュリティ強化装置。

【請求項16】前記鍵変更手段は、前記各通信装置内に保持される秘密情報、時間情報及びネットワークに固有の情報のいずれかまたは全ての組合せに基づいて前記暗号鍵を生成する、請求項2に記載のセキュリティ強化装置。

【請求項17】前記鍵変更手段は、前記各通信装置内に保持される秘密情報、時間情報及びネットワークに固有の情報のいずれかの組合せまたは全てを、一方向関数で暗号化して前記暗号鍵を生成する、請求項2に記載のセキュリティ強化装置。

【請求項18】前記利用者管理手段は、前記暗号鍵の更新及び配布を許可する鍵変更属性を、前記取得した利用者情報に基づいて設定して前記記憶手段に格納し、前記鍵変更属性の有無に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備える、請求項2に記載のセキュリティ強化装置。

【請求項19】前記利用者管理手段は、利用者が前記暗号鍵の更新及び配布を許可する鍵変更属性を有する場合に、所定の条件に基づいて他の通信装置を選択し、前記選択した通信装置に前記鍵変更属性を設定可能であり、かつ鍵変更属性の設定及び設定対象の通信装置を前記通信装置から取得して前記記憶手段に格納し、前記鍵変更属性の有無に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備える、請求項2に記載のセキュリティ強化装置。

【請求項20】前記利用者管理手段は、前記暗号鍵の更新及び配布を許可する鍵変更属性及び優先順位を、前記取得した利用者情報に基づいて設定して前記記憶手段に格納し、前記利用者情報の変化に従って前記優先順位の書き換えを行い、前記鍵変更属性及び優先順位に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備える、請求項2に記載のセキュリティ強化装置。

【請求項21】前記利用者管理手段は、利用者が前記暗号鍵の更新及び配布を許可する鍵変更属性を有する場合に、所定の条件に基づいて他の通信装置を選択し、前記他の通信装置に前記鍵変更属性と優先順位とを設定可能であり、かつ鍵変更属性と優先順位との設定及び設定対象の通信装置を前記通信装置から取得して前記記憶手段に格納し、前記利用者情報の変化に従って前記優先順位の書き

換えを行い、

前記鍵変更属性及び優先順位に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備える、

請求項2に記載のセキュリティ強化装置。

【請求項22】互いに同一のネットワークを共有して同時に双方向通信が可能な複数の通信装置から構成され、前記各通信装置は、

前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を保持する記憶手段と、通信内容を前記暗号鍵を用いて暗号化する暗号化手段と、通信内容を前記暗号鍵を用いて復号化する復号化手段と、

前記いずれかのネットワークに参加している場合に、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を取得し、前記記憶手段に格納する利用者管理手段と、

前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する鍵取得手段と、

他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布可能な鍵配布手段と、を備えるセキュリティ強化システム。

【請求項23】互いに同一のネットワークを共有して同時に双方向通信が可能な通信装置に用いられる、セキュリティ強化プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

A；前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を保持する段階と、

B；前記暗号鍵を用いて通信内容を暗号化する段階と、

C；前記暗号鍵を用いて通信内容を復号化する段階と、

D；前記いずれかのネットワークに参加している場合に、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を取得し、前記記憶手段に格納する段階と、

E；前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する段階と、

F；他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布する段階と、

を実行させるための、セキュリティ強化プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、イントラネットや

インターネットなどのコンピュータネットワーク上で行われる通信のセキュリティを高める技術に関し、なかでもチャットシステムにおける会話内容のセキュリティを高める技術に関する。本発明において、チャットシステムとは、チャットサーバと複数のチャットクライアントとから構成され、複数の利用者が互いに同一のチャンネルを共有して同時に会話可能なシステムをいう。チャンネルとは、論理的にユーザをグルーピングした仮想空間であり、チャンネル内での発言がチャンネルを共有する利用者全員にブロードキャストされる仮想空間である。ニックネームとは、チャットシステム上でユーザを識別するための名前である。チャンネルオペレータ属性とは、チャンネル内のユーザ管理及びモード管理を行う権限である。ボットとは、チャンネルに参加して様々なサービスを提供するソフトウェアロボットを言う。

【0002】

【従来の技術】従来、チャットサーバとチャットクライアントとからなるチャットシステムにおいて、チャットクライアント間の会話内容のセキュリティを高めるために、会話内容を共通鍵で暗号化することが提案されている。この共通鍵の生成方法として、例えばチャットサーバがチャンネル暗号鍵を生成し、複数のチャットクライアントに配布する方法が提供されている。

【0003】また、チャットクライアントとしてサーバに接続するボットを準備しておき、このボットにチャンネル暗号鍵を生成及び配布させ、また生成したチャンネル暗号鍵を管理させる方法も提案されている。さらに、チャットクライアントにあらかじめチャンネル暗号鍵を組み込んでおくことも考えられる。

【0004】

【発明が解決しようとする課題】前記チャットサーバがチャンネル暗号鍵を生成してチャットクライアントに配布する方法では、クライアントとサーバとの間の通信路上では会話内容の秘匿が行われる。しかし、サーバがチャンネル暗号鍵を知っているため、サーバ上で会話の解読が可能であるという問題がある。

【0005】一方、ボットを用いてチャンネル鍵を管理する方法を用いると、チャットサーバに会話内容が漏洩することはないものの、ボット上で会話内容の解読が可能である。また、サーバと別個独立したボットを運用することになり、運用上面倒である。チャットクライアントにチャンネル暗号鍵を組み込む構成は、単純ではあるものの鍵を変更できないため、鍵を解読される可能性が高くなるおそれがある。

【0006】本発明は、チャンネル暗号鍵を用いて会話の暗号化／復号化を行う場合に、チャンネル暗号鍵を管理する負担を軽減し、チャンネル鍵の解読を困難にするセキュリティ強化方法及び装置を提供することを目的とする。

【0007】

【課題を解決するための手段】前記の課題を解決するた

めに、本願第1発明は、互いに同一のネットワークを共有して同時に双方向通信が可能な通信装置に用いられ、A；ネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を、前記通信装置上で生成し、

B；通信装置を用いてネットワークに参加した後に、前記ネットワークを共有するいずれかの他の通信装置に対して前記暗号鍵を要求し、

C；ネットワーク内の他の通信装置からの暗号鍵の要求に応じ、前記準備した暗号鍵を要求元の通信装置に付与し、

D；ネットワーク内の通信装置間の通信内容を、前記暗号鍵を用いて暗号化及び復号化する、セキュリティ強化方法を提供する。

【0008】チャットシステムを例に取り説明する。例えば、チャンネル開設者により最初のチャンネル暗号鍵を生成する。次にチャンネルに参加してきたユーザは、チャンネル開設者に対してチャンネル暗号鍵を要求する。チャンネル開設者は、前記要求に応じてチャンネル暗号鍵を付与する。このように、ユーザ端末間でチャンネル暗号鍵を配布し、サーバやボット上でのチャンネル暗号鍵の解読を防止する。

【0009】本願第2発明は、他の通信装置と互いに同一のネットワークを共有して同時に双方向通信が可能な通信装置とともに用いられ、記憶手段と、暗号化手段と、復号化手段と、利用者管理手段と、鍵取得手段と、鍵配布手段とを備えるセキュリティ強化装置を提供する。記憶手段は、前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を保持する。暗号化手段は、通信内容を前記通信装置から取得し、前記暗号鍵を用いて暗号化する。復号化手段は、通信内容を前記通信装置から取得し、前記暗号鍵を用いて復号化する。

【0010】利用者管理手段は、前記通信装置が前記いずれかのネットワークに参加している場合に、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を前記通信装置から取得し、前記記憶手段に格納する。鍵取得手段は、前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する。鍵配布手段は、他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布可能である。

【0011】セキュリティ強化装置をチャットクライアントと共に用いる場合を例に取る。利用者管理手段は、チャンネルに入るとそのチャンネルに参加しているニックネームリストを含む利用者情報を、チャットクライアントを介して取得する。次に、鍵取得手段は、ニックネームリストからいずれかの他の利用者を選択し、その利用者端末にチャンネル暗号鍵を要求する。この要求を受け取っ

た他の利用者端末では、鍵配布手段が、記憶手段からチャンネル暗号鍵を取り出し、要求元の利用者端末に送信する。要求元の利用者端末は、鍵取得手段によりチャンネル暗号鍵を受け取って記憶手段に格納する。暗号化手段及び復号化手段は、前記のようにして記憶手段に格納されたチャンネル暗号鍵を用い、以降の会話内容を暗号化及び復号化する。

【0012】本願第3発明は、前記第2発明において、前記通信装置が、前記セキュリティ強化装置との連携手段を有している。さらに、連携手段は、前記暗号鍵の要求、前記要求に応じて送信される暗号鍵、前記利用者情報に関する情報及び所定の条件に合致する場合は通信内容の受け渡しを、通信装置とセキュリティ強化装置との間で行うセキュリティ強化装置を提供する。

【0013】例えば、受信した通信内容が暗号化されている場合、連携手段は、暗号化されている通信内容をセキュリティ強化装置に送出する。復号化された通信内容は連携手段を介してセキュリティ装置から通信装置に送出され、通常の会話内容と同様に表示される。逆に、通信内容を暗号化する場合、連携手段は入力された通信内容をセキュリティ強化装置に送出する。暗号化された通信内容は連携手段を介してセキュリティ強化装置から通信装置に送出され、通信装置により通常の会話内容と同様の扱いで送信される。

【0014】本願第4発明は、前記第2発明において、前記利用者管理手段が、他のセキュリティ強化装置に暗号鍵の配布を許可する鍵配布属性を、前記取得した利用者情報に基づいて設定し、前記記憶手段に格納するセキュリティ強化装置を提供する。例えば、チャットクライアントは、利用者情報としてニックネーム、ユーザID、チャンネルオペレータか否か等を取得可能である。そこで、鍵配布属性を、例えばチャンネルオペレータ属性に連動させ、チャンネルオペレータであれば鍵配布属性ありに設定する。

【0015】本願第5発明は、前記第2発明において、前記利用者管理手段が、所定の条件に基づいて、他の通信装置を選択し、前記暗号鍵の配布を許可する鍵配布属性を前記他の通信装置に付与するセキュリティ強化装置を提供する。さらに利用者管理手段は、鍵配布属性の設定及び設定対象の通信装置を前記通信装置から取得し、前記記憶手段に格納する。

【0016】たとえば、利用者管理手段は、そのチャットクライアントがチャンネル開設者である場合に、他の利用者端末を選択する。選択方法は、チャンネルに参加しているチャットクライアントからランダムに一定数選択したり、所定の参加順位までのチャットクライアントを選択するなどが挙げられる。他の利用者端末に鍵配布属性を付与可能にするために、具体的にはチャットシステムのプロトコルに新たに拡張プロトコルを設け、鍵配布属性を利用者情報として設定可能にすると良い。また、チ

ャンネルオペレータの設定と同様に、設定コマンドに基づいて鍵配布属性を付与可能にしても良い。

【0017】本願第6発明は、前記第2発明において、利用者管理手段が、他の通信装置の選択と、前記暗号鍵の配布を許可する鍵配布属性の前記他の通信装置への付与及び解除の指示とを受け付け、かつ鍵配布属性の設定及び設定対象の通信装置を前記通信装置から取得し、前記記憶手段に格納するセキュリティ強化装置を提供する。

【0018】利用者による鍵配布属性の設定及び解除を受け付け、個々の利用者端末にかかる鍵配布負担を利用者自身により調節可能にする。本願第7発明は、前記第2発明において、鍵取得手段が所定の条件に基づいて前記暗号鍵の要求先を選択するセキュリティ強化装置を提供する。すなわち、鍵取得手段は、乱数を発生させたり、鍵配布属性を有する通信装置から選択する等、所定の条件に基づいてチャンネル暗号鍵の要求先を選択する。

【0019】本願第8発明は、前記第2発明において鍵取得手段が、所定の条件に基づいて前記暗号鍵の要求先を選択して前記暗号鍵を要求し、所定時間内に前記要求先から暗号鍵が送信されない場合、他の通信装置を選択して再度要求を行うセキュリティ強化装置を提供する。要求先から一定時間内に暗号鍵が送信されてこない場合、鍵取得手段は要求先に何らかのトラブルがあったとして要求先の通信装置を選択し直す。選択基準は、ランダム、鍵配布属性のある通信装置など所定の条件を満たすものを選択する。

【0020】本願第9発明は、前記第2発明において、鍵取得手段が、前記通信内容が暗号化されている場合に前記暗号鍵の取得要求を行うセキュリティ強化装置を提供する。例えば、チャットシステムにおいて、チャンネル内の通信内容の全てを暗号化する暗号化モードを設定可能にしておく。鍵取得手段は、参加したチャンネルのモードをチャットクライアントから取得し、暗号化モードがオンである場合は暗号鍵の取得要求を行う。

【0021】本願第10発明は、前記第2発明において、前記復号化手段が、前記通信装置から受け取る通信内容を復号不可能と判断した場合、前記暗号鍵の要求を行うことを決定し、前記鍵取得手段が、前記復号化手段の決定に従い、前記暗号鍵の取得要求を行うセキュリティ強化装置を提供する。会話単位で暗号化を設定可能にすることも考えられる。例えば、GUI(Graphic User Interface)によりコマンドボタンを表示し、このコマンドボタンのオンオフにより会話毎に暗号化の設定やその解除を行う。暗号化が設定されている場合、暗号化手段は、暗号化された会話内容の先頭部分に、会話の暗号化を示す暗号化フラグを記述する。通信装置は、会話内容に送信コマンドを付加し、ネットワークに送出する。復号化手段は、暗号化された会話内容を受け取ったが暗号鍵がない場合や、保持されている暗号鍵では復号化でき

ない場合、暗号鍵を要求する旨の判断をする。鍵取得手段は、復号化手段の判断に従い、暗号鍵の取得要求を行う。

【0022】本願第11発明は、前記第2発明において、前記記憶手段が複数の暗号鍵と暗号鍵を特定する鍵識別情報とを対応付けて記憶し、前記暗号化手段が、前記通信内容の暗号化に用いられた暗号鍵を示す鍵識別情報と通信内容とを、前記通信装置を介してネットワークに送出可能であり、前記復号化手段が、前記鍵識別情報で特定される暗号鍵は前記記憶手段に保持されているか否かを判断し、前記鍵取得手段が、前記判断結果に従い、前記鍵識別情報を通知して前記暗号鍵の取得要求を行うセキュリティ強化装置を提供する。

【0023】会話毎に暗号化の設定及び解除が行われる場合に、復号化手段がその会話の暗号化に用いられたチャンネル暗号鍵を有していないと判断すれば、鍵取得手段はその判断に従ってチャンネル暗号鍵の取得要求を行う。その際には、鍵識別番号を通知することにより、どの暗号鍵を要求しているかを特定する。鍵識別番号としては、チャンネル生成時からのシリアル番号や、チャンネル暗号鍵にハッシュ関数等の一方向関数をかけたものなどが挙げられる。

【0024】本願第12発明は、前記第2発明において、前記鍵取得手段が、利用者の公開鍵暗号系の公開鍵を前記暗号鍵の要求とともに通知し、前記要求に応じて送信される暗号鍵を利用者の秘密鍵を用いて復号化し、前記鍵配布手段が、前記要求元の公開鍵暗号系の公開鍵を用いて暗号化した前記暗号鍵を配布するセキュリティ強化装置を提供する。

【0025】暗号鍵を要求する要求元の鍵取得手段は、利用者の公開鍵を通知して要求を行う。要求を受け取った通信装置の鍵配布手段は、公開鍵を用いて暗号鍵を暗号化し、送り返す。要求元では、鍵取得手段が利用者の秘密鍵を用いて復号化し、暗号鍵を取得する。本願第13発明は、前記第2発明において、前記鍵配布手段が、他の前記通信装置から前記暗号鍵の要求があった場合、前記要求を検証し、検証結果に基づいて前記記憶手段からいずれかの暗号鍵を読み出し、前記他の通信端末に配布可能であるセキュリティ強化装置を提供する。

【0026】チャンネル暗号鍵の要求を受け取った他の利用端末では、まず鍵配布手段が要求を検証する。正当な要求者であれば、鍵配布手段は、記憶手段からチャンネル暗号鍵を取り出して要求元の利用端末に送信する。前述の要求元公開鍵を用いる例では、鍵配布手段は、要求元の公開鍵が正当な公開鍵か否かを検証することが好ましい。例えば、認証局の電子署名がある公開鍵や、IRCサーバの電子署名が施された公開鍵、暗号鍵の要求を受けたユーザの電子署名がある公開鍵などを、正当な公開鍵と見なすことが挙げられる。

【0027】本願第14発明は、前記第2発明におい

て、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備えるセキュリティ強化装置を提供する。すなわち、適当なタイミングで暗号鍵を更新することにより、暗号鍵の解読を防止してセキュリティを高める。適当なタイミングとは、例えば所定の時間間隔、所定の会話数または会話量を超過したとき、ネットワークの参加利用者数が所定数を越えたときや下回ったとき、話題が変化したとき、最後の会話から所定時間経過したとき、利用者が暗号鍵の変更を指示したときなど様々なタイミングが考えられる。また、前記タイミングが生じて、会話が続行している最中に変更した鍵の配布を待機し、会話がとぎれたタイミングで鍵を再配布することも考えられる。

【0028】本願第15発明は、前記第2発明において、所定のタイミングで前記暗号鍵を更新し、前記更新した暗号鍵を直前の暗号鍵を用いて暗号化して他の通信装置に配布する鍵変更手段をさらに備えるセキュリティ強化装置を提供する。前記更新された暗号鍵をその更新前の暗号鍵を用いて暗号化することにより、更新された暗号鍵を配布する際の解読のおそれを防止する。

【0029】本願第16発明は、前記第2発明において、前記鍵変更手段が、前記各通信装置内に保持される秘密情報、時間情報及びネットワークに固有の情報のいずれかまたは全ての組合せに基づいて前記暗号鍵を生成するセキュリティ強化装置を提供する。例えば、通信装置内に記憶されている基板番号やプログラムの格納アドレス、暗号鍵を更新する時間、チャンネル名及びチャンネルパスワードに基づいて、新たな暗号鍵を生成することが考えられる。

【0030】本願第17発明は、前記第2発明において、前記鍵変更手段が、前記各通信装置内に保持される秘密情報、時間情報及びネットワークに固有の情報のいずれかの組合せまたは全てを、一方向関数で暗号化して前記暗号鍵を生成するセキュリティ強化装置を提供する。例えば、通信装置内に記憶されている基板番号やプログラムの格納アドレス、暗号鍵を生成する時間、チャンネル名及びチャンネルパスワードを、ハッシュ関数で暗号化して暗号鍵とする。

【0031】本願第18発明は、前記第2発明において、前記利用者管理手段が、前記暗号鍵の更新及び配布を許可する鍵変更属性を、前記取得した利用者情報に基づいて設定して前記記憶手段に格納し、前記鍵変更属性の有無に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備えるセキュリティ強化装置を提供する。

【0032】前記鍵配布属性と同様、鍵変更属性をチャンネルオペレータ属性に連動させて設定したり、チャンネルに最後まで参加している利用者に設定してもよい。また、新たに拡張プロトコルを設けてチャットシステム上で鍵変更属性を設定可能にし、鍵変更属性を利用者情報



として取得するようにしても良い。さらに、チャネルオペレータからの設定コマンドに基づいて鍵変更属性を設定することも可能である。

【0033】本願第19発明は、前記第2発明において、前記利用者管理手段が、利用者が前記暗号鍵の更新及び配布を許可する鍵変更属性を有する場合に、所定の条件に基づいて他の通信装置を選択し、前記選択した通信装置に前記鍵変更属性を設定可能である。かつ、利用者管理手段は、鍵変更属性の設定及び設定対象の通信装置を前記通信装置から取得して前記記憶手段に格納する。さらに、前記鍵変更属性の有無に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備えるセキュリティ強化装置である。

【0034】鍵変更属性を有する利用者は、他の利用者に対して鍵変更属性を付与可能にしても良い。他の利用者の選択方法は、ランダムに一定数の通信装置を選択したり、チャネルへの参加順序に応じて一定数の通信装置を選択したり、任意の通信装置を通信装置リストから選択したり、様々である。鍵変更属性の設定は、例えばチャットシステム上で新たなコマンドを設定することにより可能になる。この設定に応じて、チャネルに参加しているユーザ端末は、ユーザ情報の書き換えをそれぞれ行う。

【0035】本願第20発明は、前記第2発明において、前記利用者管理手段が、前記暗号鍵の更新及び配布を許可する鍵変更属性及び優先順位を、前記取得した利用者情報に基づいて設定して前記記憶手段に格納し、前記利用者情報の変化に従って前記優先順位の書き換えを行う。さらに、鍵変更属性及び優先順位に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備えるセキュリティ強化装置である。

【0036】例えば、チャネルオペレータ属性に基づいて鍵変更属性を、チャネルへの参加順序に基づいて優先順位を設定する。第2位以降の利用者管理手段は、第1位の通信装置がネットワークから退出した場合や、前回の暗号鍵の更新から所定時間が経過して第1位の通信装置に何らかのトラブルがあったと判断する場合、利用者情報に基づいて自動的に優先順位をひとつづつ繰り上げる。新たな鍵の生成は、第1位のユーザが、所定のタイミングで行う。

【0037】本願第21発明は、前記第2発明において、前記利用者管理手段が、利用者が前記暗号鍵の更新及び配布を許可する鍵変更属性を有する場合に、所定の条件に基づいて他の通信装置を選択し、前記他の通信装置に前記鍵変更属性と優先順位とを設定可能である。かつ、利用者管理手段は、鍵変更属性と優先順位との設定及び設定対象の通信装置を前記通信装置から取得して前記記憶手段に格納し、前記利用者情報の変化に従って前

記優先順位の書き換えを行う。さらに、このセキュリティ強化装置は、前記鍵変更属性及び優先順位に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備えている。

【0038】例えば、チャネル暗号鍵の変更及び配布は、第1位の通信装置が行う。第2位以下の通信装置は、第1位の通信装置が配布する新たなチャネル暗号鍵を取得する。第2位以降の利用者管理手段は、第1位の通信装置がネットワークから退出した場合や、前回の暗号鍵の更新から所定時間が経過して第1位の通信装置に何らかのトラブルがあったと判断する場合、利用者情報に基づいて自動的に優先順位をひとつづつ繰り上げる。新たに第1位となった通信装置は、自ら暗号鍵の変更及び配布を行う。

【0039】本願第22発明は、互いに同一のネットワークを共有して同時に双方向通信が可能な複数の通信装置から構成され、前記各通信装置が、記憶手段と、暗号化手段と、復号化手段と、利用者管理手段と、鍵取得手段と、鍵配布手段とを備えるセキュリティ強化システムを提供する。記憶手段は、前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を保持する。

【0040】暗号化手段は、通信内容を前記暗号鍵を用いて暗号化する。復号化手段は、通信内容を前記暗号鍵を用いて復号化する。利用者管理手段は、前記いずれかのネットワークに参加している場合に、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を取得し、前記記憶手段に格納する。鍵取得手段は、前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する。鍵配布手段は、他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布可能である。

【0041】前記第2発明と同様の作用効果を有する。本願第23発明は、互いに同一のネットワークを共有して同時に双方向通信が可能な通信装置に用いられる、セキュリティ強化プログラムを記録したコンピュータ読み取り可能な記録媒体であって、下記A～F段階を実行させるためのセキュリティ強化プログラムを記録した、コンピュータ読み取り可能な記録媒体を提供する。

A：前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を保持する段階、

B：前記暗号鍵を用いて通信内容を暗号化する段階、

C：前記暗号鍵を用いて通信内容を復号化する段階、

D：前記いずれかのネットワークに参加している場合に、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を取得し、前記記憶手段に格納する段階、

E: 前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する段階、

F: 他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布する段階。

【0042】前記第2発明と同様の作用効果を有する。

【0043】

【発明の実施の形態】次に、本発明のセキュリティ強化装置について、実施形態例を挙げて具体的に説明する。以下の実施形態例においては、チャットシステムにおける会話内容のセキュリティを高めるために、本発明のセキュリティ強化装置をチャットクライアントとともに用いる場合を例に取り、説明する。

【0044】＜第1実施形態例＞図1に、チャットクライアントと共に用いられるセキュリティ強化装置の機能構成図を示す。図1において、複数のユーザ端末A、B、C、D、E…は、チャットクライアントが動作可能であり、チャットサーバとコンピュータネットワークを介して接続されている。セキュリティ強化装置1は、チャットクライアントとともに、各ユーザ端末に設けられている。

【0045】セキュリティ強化装置1は、記憶部2、ユーザ管理部3、鍵取得部4、鍵配布部5、鍵変更部6、鍵生成部7及び暗号化／復号化部8を有している。チャットクライアント10には、セキュリティ強化装置1に依り、ユーザDB9、連携部11及び振り分け部12が設けられている。本実施形態例においては、セキュリティ強化装置1及びチャットクライアント10を有する複数のユーザ端末A～E間において、会話を暗号化／復号化するためのチャンネル暗号鍵を生成し、配布する。

【0046】【セキュリティ強化装置】記憶部2は、ユーザ自身の公開鍵系秘密鍵及び公開鍵を記憶している。また、記憶部2は、チャットクライアントが参加しているチャンネルにおける会話を暗号化／復号化するためのチャンネル暗号鍵を、鍵取得部4から受け取り、保持する。さらに、記憶部2は、チャンネル暗号鍵を特定する暗号鍵IDを鍵取得部4から受け取り、チャンネル暗号鍵と暗号鍵IDとを対応付けて暗号鍵リストに保持する。記憶部2に保持されるチャンネル暗号鍵は、1つとは限らず複数でも良い。複数のチャンネル暗号鍵が保持される場合には、記憶部2に保持するチャンネル暗号鍵の最大数を予め設定またはユーザにより設定可能にしておくことが望ましい。

【0047】ユーザ管理部3は、チャットクライアントがチャットサーバから取得するユーザ情報を参照し、参照したユーザ情報に基づいて、鍵配布属性及び鍵変更属性を設定する。図2に、鍵配布属性及び鍵変更属性を含めたユーザ情報の一例を示す。ここで、鍵配布属性とは、チャンネル暗号鍵を他のユーザ端末に配布することが

許可されていることを示す。また、鍵変更属性とは、チャンネル暗号鍵を新たに更新し、他のユーザ端末に配布することが許可されていることを示す。

【0048】通常、チャットクライアントは、チャンネルに参加することにより所定のユーザ情報をサーバから取得可能である。取得可能なユーザ情報としては、(1)ニックネーム、(2)ユーザの実際の氏名であるReal Name、(3)ネットワーク上でユーザを特定するためのユーザID、(4)チャットクライアントが動作している利用端末を特定するクライアント名、(5)利用端末が接続しているサーバを特定するサーバ名、(6)各ユーザが接続しているチャンネルのリスト、(7)最終発言からの経過時間、(8)チャンネルオペレータ属性の有無(0/1)などが挙げられる。このうち、少なくともニックネームは、チャンネル内のユーザを特定するために必要な情報である。

【0049】図2に示したユーザ情報の例では、チャットクライアントは、前記(1)～(8)のユーザ情報をチャットサーバから取得してユーザDBに書き込む。ユーザ管理部3は、チャットクライアントが取得したユーザ情報の中のチャンネルオペレータ属性に基づいて鍵配布属性及び鍵変更属性を設定し、ユーザDB9に書き込んでいる。チャンネルオペレータ属性が"1"であれば、鍵配布属性及び鍵変更属性もそれぞれ"1"に設定される。また、ユーザ管理部3は、ユーザ情報の変化、例えば新たなチャンネルオペレータの設定やユーザの退出を、後述するチャットクライアントの連携部11を介して通知され、変化に応じてユーザ情報を更新する。

【0050】鍵配布属性や鍵変更属性の設定方法は、他にも考えられる。属性の他の設定方法として、ユーザ管理部3により所定の条件に基づいてユーザを選択し、選択したユーザに属性を設定する方法があげられる。鍵配布属性の付与対象の選択方法としては、例えば、乱数を発生させることによりランダムに一定数のユーザを選択したり、チャンネルへの所定の参加順位までのユーザを手動あるいは自動的に選択したり、ユーザによる他のユーザの指定を受け付けることにより選択することが挙げられる。

【0051】鍵変更属性の付与対象の選択方法としては、例えば、チャンネルの開設者を選択したり、チャンネルに最後まで参加していたユーザを選択したりすることが挙げられる。また、鍵変更属性を有するユーザにより、例えば、チャンネルへの参加順序に応じて一定数のユーザを選択したり、ランダムに一定数のユーザを選択したり、ユーザの手動による他のユーザの指定を受け付けて選択することが挙げられる。

【0052】これら選択したユーザに対し、属性を設定する方法の一つとして、属性配布コマンドを新たに設けることが考えられる。例えば、鍵配布属性の設定コマンドを"MODE #CH1 +d userA"、鍵変更属性の設定コマンドを"MODE #CH1 +x userA"とする。但し、ここで#CH1は任

意のチャンネル名、userAは任意のチャンネル内ユーザのニックネームとする。ユーザ管理部3により、選択されたユーザ及び配布する属性を指定して前記コマンドをチャットクライアントに送出することにより、チャンネルに参加している全ユーザ端末に前記コマンドが通知される。他のユーザ端末では、チャットクライアントを介してコマンドを受け取ったユーザ管理部3が、コマンドを解釈してユーザ情報の書き換えを行う。

【0053】複数のユーザが鍵変更属性を有する場合、ユーザ管理部3によりチャンネル暗号鍵を変更する優先順位を併せて設定することが好ましい。例えば、チャンネルオペレータ属性に連動させて鍵変更属性を設定する場合は、チャンネル開設者の優先順位を第1位とし、他のユーザの優先順位はチャンネルに参加した順に設定する。また、鍵変更属性を有するユーザが一人であり、そのユーザから他のユーザに鍵変更属性を付与する場合は、最初に鍵変更属性を有していたユーザの優先順位を第1位とする。そして、ユーザ管理部3により選択されるユーザに対し、チャンネルへの参加順序に応じて、ランダムに、または手動による指定を受け付け、優先順位を設定する。

【0054】前記優先順位を設定するために、前記属性設定コマンドにより属性と共に優先順位の設定も可能にしておくことが好ましい。例えば、鍵変更属性の設定コマンドにおいて、拡張子"+x"のあとに優先順位を示す自然数"n"を記述することにより、優先順位を設定することが考えられる。例えば、"userA"に第2位の鍵変更属性を設定するコマンドは、"MODE #CH1 +x2 userA"となる。鍵変更属性と共に設定される優先順位は、チャンネル内の全てのユーザ端末に通知される。従って、各ユーザ端末のユーザ管理部3は、ユーザ情報の変化、例えばいずれかのユーザが退出することにより鍵変更属性の優先順位に変更が生じると、生じた変化に応じて優先順位を書き換えることが出来る。

【0055】鍵取得部4は、所定の条件に基づいて、他のユーザの選択及び選択したユーザへのチャンネル暗号鍵の要求を行う。また、要求に応じて送信されてくるチャンネル暗号鍵を記憶部2に格納する。チャンネル暗号鍵の要求先の選択方法は特に限定されない。例えば、乱数を発生させることによりランダムに一意のユーザを選択したり、鍵配布属性を有するユーザからチャンネルに参加した順に選択することが挙げられる。選択したユーザ端末が多忙であったり、通信路が混雑しているなど、何らかの事情により選択したユーザ端末から一定時間経過しても応答がない場合、鍵取得部4は、他のユーザ端末を選択し、再びチャンネル暗号鍵の要求を行う。

【0056】チャンネル暗号鍵の要求は、所定の情報及びユーザ証明書を送信することにより行う。所定の情報とは、チャンネル名と、ニックネームなどの要求元ユーザを特定する情報とを最低限含んでいる。ユーザ証明書は、

ユーザに関する情報、すなわち証明書本体と、要求元ユーザの公開鍵と、証明者である認証局の電子署名とから構成されている。証明者としては、認証局が一般的ではあるが、他にユーザ端末が接続するサーバや、鍵を要求する先のユーザなどでも良い。

【0057】前記チャンネル暗号鍵の要求を行うタイミングは、鍵取得部4が通信の暗号化を確認したときである。具体的には、そのチャンネル内の通信が全て暗号化されている暗号化モードを確認したとき、または暗号化された会話を受信したときである。前者の場合、チャンネル内の全会話を暗号化する暗号化モードの設定コマンドを予め準備しておく。例えば、"MODE #CH1 +c"などのように、"MODE"コマンドの拡張子を用いたコマンドを準備する。通常、チャットクライアントがチャンネルに参加すると、そのチャンネルに設定されているモードが通知される。鍵取得部4は、このモードをチャットクライアントの連携部11から取得し、暗号化モードであればチャンネル暗号鍵の要求を行う。

【0058】後者の場合、会話毎にその会話が暗号化されているか否かを示す暗号化フラグを、各会話と共に送信することが考えられる。通常のチャットシステムにおいては、会話を送信する送信コマンドと会話内容とからなる会話メッセージが作成される。本実施形態例においては、さらに暗号化のオン/オフを示す暗号化フラグ(0/1)を会話内容の先頭部分に記述して会話メッセージを作成する。

【0059】また、暗号化フラグに代えて暗号鍵IDを用いることも考えられる。暗号化フラグを会話内容に記述することは、後述するように暗号化/復号化部8が行う。鍵取得部4は、暗号化/復号化部8がチャットクライアントから受け取る会話内容を復号化できない場合、後述する暗号化/復号化部8の指示に従ってチャンネル暗号鍵の要求を行う。暗号化/復号化部8が復号化を行えない場合については後述する。

【0060】鍵取得部4は、要求元ユーザの公開鍵で暗号化されたチャンネル暗号鍵を受信し、これをユーザの秘密鍵で復号化してチャンネル暗号鍵を取得する。また、暗号化されたチャンネル暗号鍵と共に暗号鍵IDを受信し、取得したチャンネル暗号鍵と暗号鍵IDとを記憶部2の暗号鍵リストに格納する。さらに、鍵取得部4は、ユーザ端末に鍵変更属性がない場合か、鍵変更属性を有していても優先順位が第1位でない場合には、他のユーザ端末から送信される新たなチャンネル暗号鍵を取得する。取得した新たなチャンネル暗号鍵は直前のチャンネル暗号鍵を用いて暗号化されているので、鍵取得部4は、直前のチャンネル暗号鍵を記憶部2から取り出し、送信されてきたチャンネル暗号鍵を復号化する。また、前記と同様に、復号化したチャンネル暗号鍵から暗号鍵IDを求め、チャンネル暗号鍵と対応付けて暗号鍵リストに格納する。さらに、鍵取得部4は、チャンネル暗号鍵が更新される所定のタイ

ミングを経過しても新たなチャンネル暗号鍵を受信しない場合、ユーザ管理部3に対して優先順位の変更の指示を通知する。この通知を受け、ユーザ管理部3により鍵変更属性の優先順位の繰り上げが行われる。チャンネル暗号鍵の更新については後述する。

【0061】鍵配布部5は、他のユーザ端末から送信されるチャンネル暗号鍵の要求を検証する。要求の検証には、チャンネル暗号鍵の要求とともに要求元から送信されるユーザ証明書を用いる。検証の結果、要求元が正当なユーザであることを判断すると、最新のチャンネル暗号鍵を暗号鍵リストから取り出し、ユーザ証明書に含まれる要求元の公開鍵で暗号化する。鍵配布部5は、前記取り出したチャンネル暗号鍵にハッシュ関数などの一方向関数をかけて暗号鍵IDを求め、暗号化したチャンネル暗号鍵と暗号鍵IDとを要求元に送信する。暗号鍵IDはチャンネル暗号鍵を一義的に特定できればよいので、シリアル番号やチャンネル暗号鍵を生成した日付及び時刻などを暗号鍵IDとして用いても良い。また、鍵配布部5は、要求とともに暗号鍵IDが送信された場合は、暗号鍵IDにより指定されるチャンネル暗号鍵を送信する。

【0062】鍵変更部6は、適当なタイミングでチャンネル暗号鍵を新たに生成し、生成したチャンネル暗号鍵を他のユーザ端末に送信する。新たにチャンネル暗号鍵を生成するタイミングとしては、例えば一定時間経過毎に生成することが挙げられる。また、チャットクライアントにおける会話数や会話のデータ量を監視することにより、ある一定会話数毎に、あるいは一定会話量毎に生成してもよい。さらに、ユーザ情報を監視して、チャンネル内ユーザ数が所定数、例えば1になったとき、チャンネルのトピックが変化したとき、最後の会話から所定時間経過したとき、ユーザがチャンネル暗号鍵の変更を指示する任意の時など、様々なタイミングが考えられる。鍵変更部6は、生成したチャンネル暗号鍵をすぐに送信しても良いが、会話が断続的に続いているような状態では送信を見合わせ、会話がとぎれたときに送信を行うようにすると好ましい。

【0063】新たなチャンネル暗号鍵の生成は、例えばユーザ端末内に保持されている秘密情報、時間情報、チャンネル固有情報などの情報を組み合わせ、ハッシュ関数などの一方向関数をかけることにより生成するとよい。ユーザ端末内に保持されている秘密情報とは、端末内の基板の製造番号や、ある特定のプログラムのアドレスなど、第3者が容易に想到しにくい情報が好ましく、さらに時間的に静的情報ではなく変化する情報であればさらに好ましい。

【0064】時間情報としては、前記チャンネル暗号鍵の生成タイミングにおける時刻データを、時刻データ取得プログラムルーチンを用いて取得する。時刻データ取得プログラムルーチンは、ユーザ端末の内部時計を利用し

システムにより提供されている。時刻データとしては、時刻データ取得プログラムルーチンが出力する1970年1月1日からの通算秒が一般に用いられる。チャンネル固有情報としては、例えばチャンネル名やチャンネルに設定されているパスワードなどが挙げられる。

【0065】生成した新たなチャンネル暗号鍵は、そのまま送信するよりも、暗号化して送信する方がセキュリティの観点から好ましい。例えば、1つ前のチャンネル暗号鍵を用いて新たなチャンネル暗号鍵を暗号化して送信すると、受信側も復号可能である上に盗聴を防止しやすいと考えられる。前記チャンネル暗号鍵の生成及び配布は、ユーザ情報の鍵変更属性に基づいて行うことが好ましい。すなわち、ユーザ情報の鍵変更属性が付与されている場合のみ、前記チャンネル暗号鍵を生成し、配布する。鍵変更属性は、前述のように各ユーザ端末においてユーザ管理部3により設定される。鍵変更属性とともに優先順位が設定されている場合は、例えば次のようにしてチャンネル暗号鍵の更新を行う。

【0066】優先順位が第1位のユーザにおいては、鍵変更部6は前述のように所定のタイミングで新たなチャンネル暗号鍵を生成し、他のユーザ端末に送信する。優先順位が第2位以降のユーザにおいては、所定時間経過しても新たなチャンネル暗号鍵が送信されてこない場合、第1位のユーザ端末が何らかの事情でチャンネル暗号鍵を送信できなかったものと判断する。この判断は、前述のように鍵取得部4で行う。そして、ユーザ管理部3により順次優先順位の繰り上げが行われた結果新たに第1位となったユーザが、チャンネル暗号鍵の生成及び配布を行う。

【0067】鍵生成部7は、チャットクライアントがチャンネル開設者である場合、最初のチャンネル暗号鍵を生成する。生成方法は、前記チャンネル暗号鍵の更新と同様に、ユーザ端末内の秘密情報、時間情報、チャンネル固有情報などの情報を組み合わせ、ハッシュ関数をかけて生成するとよい。時間情報としては、例えばチャンネルを開設した時刻のデータを用いるなどが考えられる。また、鍵生成部7は、生成したチャンネル暗号鍵にハッシュ関数をかけるなどして前述の鍵配布部5と同様に暗号鍵IDを作成し、チャンネル暗号鍵と暗号鍵IDとを対応付けて記憶部2に格納する。

【0068】暗号化／復号化部8は、後述するチャットクライアントの振り分け部12から暗号化された会話内容が送出されることに従い、記憶部2に保持されているチャンネル暗号鍵を取り出し、会話内容の復号化を行う。復号化に用いるチャンネル暗号鍵には通常は最新のチャンネル暗号鍵を用いるが、会話内容の先頭に暗号鍵IDが記述されている場合、暗号鍵IDにより特定されるチャンネル暗号鍵を用いて復号化を行う。

【0069】また、暗号化／復号化部8は、復号化を行うことができない場合、鍵取得部4に対し鍵要求を行う

ことを指示する。復号化を行うことができない場合は、(1)記憶部2にチャンネル暗号鍵が保持されていない場合または(2)通知された暗号鍵IDに対応するチャンネル暗号鍵が記憶部2に保持されていない場合である。復号化した会話内容は、再びチャットクライアントに送出され、通常のメッセージを受信した場合と同様に画面上に表示される。

【0070】さらに、暗号化／復号化部8は、振り分け部12から会話内容を受け取ると、最新のチャンネル暗号鍵を用いて暗号化する。ついで、暗号化した会話内容の先頭部分に暗号化フラグまたは暗号鍵IDを記述し、再びチャットクライアントに送出する。チャットクライアントでは、通常の会話内容と同様に、セキュリティ強化装置1から送出されたデータに送信コマンドを付加し、送信する。

【0071】【チャットクライアント】図1に示すように、本実施形態例におけるチャットクライアント10には、連携部11と振り分け部12とがセキュリティ強化装置1に応じて設けられている。連携部11は、チャットクライアントが送受信するコマンドを解釈し、セキュリティ強化装置1の各構成要素に処理を振り分ける。具体的には、連携部11は、ユーザ情報が変化するコマンドを解釈すると、ユーザ情報の変化及びその内容をユーザ管理部3にユーザ管理部3に通知する。前記コマンドとしては、例えばユーザの退出を示すコマンド"PART"、参加を示すコマンド"JOIN"、チャンネルオペレータの特権を授与するコマンド"MODE #CH1 +o"、鍵配布属性の設定コマンド"MODE #CH1 +d userA"、鍵変更属性及び優先順位の設定コマンド"MODE #CH1 +xn userA"等が挙げられる。また、逆に、ユーザ管理部3からの鍵配布属性の設定コマンド"MODE #CH1 +d userA"、鍵変更属性及び優先順位の設定コマンド"MODE #CH1 +xn userA"等を受け付け、処理する。

【0072】連携部11は、チャンネル暗号鍵の授与を示すコマンドや暗号化モードの設定コマンドを解釈すると、鍵取得部4に対し通知する。また、鍵取得部4からチャンネル暗号鍵の取得を要求するコマンドを受け付け、処理する。連携部11は、チャンネル暗号鍵の要求を示すコマンドを解釈すると、鍵配布部5に対し要求を通知する。また、鍵配布部5からの要求に対してチャンネル暗号鍵の授与コマンドを受け付け、処理する。

【0073】振り分け部12は、送信されてきた会話メッセージの先頭部分が暗号化フラグ"1"または暗号鍵IDである場合、復号化の指示を暗号化／復号化部8に通知する。具体的には、暗号化フラグまたは暗号鍵IDと暗号化された会話内容とを暗号化／復号化部8に送出する。また、振り分け部12は、利用者からの暗号化の指示及び解除を受け付け、暗号化が指示されている場合には、入力された会話内容を暗号化／復号化部8に送出する。暗号化の指示及び解除は、例えばGUI(Graphic U

ser Interface)を利用してコマンドボタンを画面上に表示させ、コマンドボタンのオン／オフによりなされるようにすることが出来る。さらに、振り分け部12は、暗号化／復号化部8により暗号化され、暗号化フラグまたは暗号鍵IDを含む会話内容を、通常の会話内容と同様に処理する。すなわち、暗号化された会話内容は、チャットクライアントにより通常の会話内容と同様に、送信コマンドを付加され、通常のチャットシステムにおける発言として送信される。

【0074】【処理の流れ】次に、セキュリティ強化装置1が行う主な処理の流れを説明する。図3は、セキュリティ強化装置1が行うメインルーチンの処理の流れを示すフローチャートである。図4～6は、メインルーチンにおいて行われる処理の詳細を示している。図4は、他のユーザ端末から鍵を取得するための鍵取得処理の流れを示すフローチャート、図5は、他のユーザ端末に鍵を配布する鍵配布処理の流れを示すフローチャート、図6は、他のユーザからの鍵の要求を検証する要求検証処理の流れを示すフローチャートである。また、図7は、メインルーチンと独立に行われ、所定の条件に従ってチャンネル暗号鍵を変更する場合の鍵変更処理の流れを示すフローチャートである。

【0075】(1)メインルーチン

ユーザ端末においてチャットクライアントがチャンネルに参加またはチャンネルを開設することにより、図3のメインルーチンの処理が開始される。説明を容易にするため、鍵配布属性及び鍵変更属性をチャンネルオペレータに連動させて設定する場合を例に取り、説明する。

【0076】ステップS1では、ユーザ管理部3が、ユーザ情報のチャンネルオペレータに連動させて、鍵配布属性及び鍵変更属性を設定する。ステップS2では、ユーザ管理部3は、ユーザがチャンネルの開設者か否かを判断する。チャンネル内のユーザが1人だけ、すなわちチャンネルに参加しているチャットクライアントが自己のチャットクライアントだけであれば、そのユーザはチャンネル開設者であるのでステップS3に移行する。チャンネルの開設者ではなく複数のユーザがチャンネル内にいれば、チャンネル暗号鍵を取得するためにステップS4に移行する。

【0077】ステップS3では、チャンネル開設者のユーザ端末において、鍵生成部7がチャンネル暗号鍵を生成する。さらに、生成したチャンネル暗号鍵に暗号鍵IDを付し、記憶部2の暗号鍵リストに格納し、ステップS5に移行する。ステップS4では、チャンネル開設者ではないユーザが、後述する鍵取得サブルーチンにより他のユーザ端末に対してチャンネル暗号鍵の要求を行い、チャンネル暗号鍵を取得する。ステップS5では、後述する鍵配布サブルーチンにより、鍵配布属性を有するユーザが他のユーザ端末にチャンネル暗号鍵を配布する。

【0078】ステップS6では、当該チャットクライアントがチャンネルから退出するか否かを判断し、退出する

のであれば処理を終了する。退出しないのであれば、再びステップS5に戻り、他のユーザからの要求に応じてチャンネル暗号鍵を配布する。なお、図示していないが、ユーザ管理部3は、メインルーチンとは独立にチャットクライアントからのユーザ情報の変更の通知を受け付け、通知に従って鍵配布属性及び鍵変更属性をを更新している。

#### 【0079】(2) 鍵取得処理

次に、前記メインルーチンのステップS4で行う鍵取得処理について、図4を参照しながら説明する。まず、ステップS11では、鍵取得部4が、暗号化モードの設定になっているかどうかを判断する。暗号化モードであれば、会話内容は全て暗号化されており、チャンネル暗号鍵を取得する必要があるため、後述するステップS13に移行する。暗号化モードでなければステップS12に移行する。

【0080】ステップS12では、鍵取得部4は、暗号化／復号化部8から鍵の取得を指示されているかどうかを判断する。チャンネル暗号鍵を取得していない状態で暗号化フラグが“1”のまたは暗号鍵IDを含む会話メッセージを受信した場合、暗号化／復号化部8は鍵取得部4に対して鍵の取得を指示するからである。ステップS12では、暗号化／復号化部8からの指示を待機し、指示があるとステップS13に移行する。

【0081】ステップS13では、鍵取得部4が、他のユーザを選択するための乱数を発生させる。ステップS14では、鍵取得部4が、発生させた乱数に基づいて、鍵配布属性を有する他のユーザの中からいずれかのユーザを選択する。ステップS15では、鍵取得部4が、記憶部2からユーザの公開鍵を取り出し、チャンネル名及びニックネームにユーザの公開鍵を含むユーザ証明書を添付し、チャンネル暗号鍵の要求を送信する。前述のように、鍵取得部4は、暗号鍵IDを含む会話メッセージの受信に応じてチャンネル暗号鍵を要求する場合には、暗号鍵IDを指定して要求を送信する。逆に、暗号化モードの通知または暗号化フラグが“1”の会話メッセージの受信に応じて要求を行う場合には、暗号鍵IDを指定せずに要求を送信する。

【0082】ステップS16では、鍵取得部4が、チャンネル暗号鍵及び暗号鍵IDを受信したかどうか判断し、まだであればステップS17に移行する。受信していればステップS18に移行する。ステップS17では、鍵取得部4が、所定時間Tが経過しているかどうかを判断し、まだであればステップS16に戻ってチャンネル暗号鍵の受信を待機する。所定時間Tが経過していれば、鍵取得部4は、選択したユーザが何らかの理由によりチャンネル暗号鍵を送信できないものと判断し、他のユーザ端末を再度選択すべくステップS13に戻る。

【0083】ステップS18では、鍵取得部4が、受信した暗号鍵をユーザの公開鍵を用いて復号化してチャネ

ル暗号鍵を得、チャンネル暗号鍵と共に受信した暗号鍵IDとともに暗号鍵リストに格納し、処理を終了する。

#### (3) 鍵配布処理

次に、前記メインルーチンのステップS5で行う鍵配布処理について、図5を参照しながら説明する。

【0084】まず、ステップS21では、鍵配布部5が、ユーザ情報を参照し、自己のユーザ端末に鍵配布属性があるかどうかを判断する。鍵配布属性がなければ処理を終了し、あればステップS22に移行する。ステップS22では、鍵配布部5が、他のユーザ端末からのチャンネル暗号鍵の要求を受け取ったかどうかを判断する。受け取っていればステップS23に移行し、受け取っていない場合は、要求を受け取るまで待機する。

【0085】ステップS23では、鍵配布部5が、後述する要求検証サブルーチンを実行し、要求の送信元が正当なユーザかどうかを検証して検証結果を得る。ステップS24では、鍵配布部5が、検証結果に基づき要求元ユーザが正当なユーザかどうかを判断し、正当でなければステップS25に移行する。正当なユーザであれば、ステップS26に移行する。

【0086】ステップS25では、鍵配布部5が、正当でないユーザに対して例えばチャンネル暗号鍵を配布できない旨のメッセージを送信するなどの適当な処理を行う。ステップS26では、要求元が正当なユーザであったので、鍵配布部5は、チャンネル暗号鍵の要求とともに送られて来ているユーザ証明書から要求元ユーザの公開鍵を取り出す。

【0087】ステップS27では、鍵配布部5が、最新のチャンネル暗号鍵を暗号鍵リストから取り出す。要求と共に暗号鍵IDが送信されてきている場合は、暗号鍵IDにより特定されるチャンネル暗号鍵を取り出す。また、取り出したチャンネル暗号鍵にハッシュ関数をかけて暗号鍵IDを求める。ステップS28では、鍵配布部5が、前記チャンネル暗号鍵を要求元ユーザの公開鍵で暗号化する。

【0088】ステップS29では、鍵配布部5が、暗号化されたチャンネル暗号鍵及び暗号鍵IDを、チャットクライアントを介して要求元ユーザ端末に送信し、メインルーチンに戻る。

#### (4) 要求検証処理サブルーチン

次に、前記鍵配布サブルーチンのステップS23で行う要求検証処理について、図6を参照しながら説明する。

【0089】ステップS31では、鍵配布部5が、チャンネル暗号鍵の要求とともに送信されてきたユーザ証明書を取り出す。ステップS32では、鍵配布部5が、ユーザ証明書の中の認証局の電子署名を取り出す。ステップS33では、鍵配布部5が、前記取り出した電子署名を、通常ユーザ端末が有する認証局データベースのなかから検索する。

【0090】ステップS34では、鍵配布部5が、前記

検索の結果に基づいて電子署名が認証局DBに登録されているか否かを判断し、登録されていなければステップS391に移行する。登録されていなければステップS35に移行する。ステップS35では、鍵配布部5が認証局の公開鍵を認証局DBから取得する。

【0091】ステップS36では、鍵配布部5が、前記電子署名を認証局の公開鍵で復号化し、ユーザ証明書のメッセージダイジェスト(MD)を求める。ステップS37では、鍵配布部5が、前記ユーザ証明書のうち、前記電子署名の対象となっている部分を取り出し、通常用いられるアルゴリズムを用いてメッセージダイジェスト(MD')を計算する。通常用いられるアルゴリズムとしては、例えばMD5やSHAなどが挙げられる。

【0092】ステップS38では、鍵配布部5が、2つのメッセージダイジェストを比較し、両者が一致していればステップS39に移行する。一致しなければステップS391に移行する。ステップS39では、鍵配布部5が「要求元ユーザは正当である」旨を検証結果とする。

【0093】ステップS391では、鍵配布部5が、要求元ユーザを不当なユーザとして扱い、例えば要求元ユーザに不当である旨の通知を送出する。

#### (5) 鍵変更処理

次に、前記メインルーチンと平行して独立に行われる鍵変更処理について、図7を参照しつつ説明する。

【0094】まず、ステップS41では、鍵変更部6が、当該ユーザ端末に鍵変更属性があるか否かを、ユーザ情報を参照して判断する。鍵変更属性がないと判断すると、後述するステップS50に移行する。鍵変更属性があると判断すると、ステップS42に移行する。ステップS42では、鍵変更部6が、当該ユーザ端末に鍵変更属性とともに付与されている優先順位が第1位か否かを判断する。第1位であればステップS43に移行し、第2位以降であれば後述するステップS50に移行する。

【0095】ステップS43では、鍵変更部6が所定のトリガの発生を待機し、所定のトリガが発生すると、ステップS44に移行する。今、説明を分かりやすくするために、チャンネル内ユーザが1人になったときまたは所定時間毎に、チャンネル暗号鍵を変更するものとする。具体的には、チャンネル内ユーザが最後の1人になった場合、またはチャンネル内に複数のユーザがいても前回の更新から所定時間が経過している場合に、ステップS44に移行する。

【0096】ステップS44では、鍵変更部6が、予め決めておいた規則により暗号鍵を生成する。例えば、ユーザ端末において本プログラムが格納されているアドレス、前記トリガが発生した時刻、チャンネル名及びチャンネルのパスワードの組合わせにハッシュ関数をかけたものを新たなチャンネル暗号鍵とする。また、新たなチャネ

ル暗号鍵にハッシュ関数をかけて暗号鍵IDを求める。

【0097】ステップS45では、鍵変更部6が、直前のチャンネル暗号鍵を暗号鍵リストから取得する。ステップS46では、鍵変更部6が、生成した新たな暗号鍵を直前のチャンネル暗号鍵で暗号化する。ステップS47では、鍵変更部6が、暗号化した新たなチャンネル暗号鍵の送信を行うか否かを、現在の会話状況に基づいて判断する。例えば、最後の発言から所定時間経過していれば、会話がとぎれていると判断してステップS48に移行する。所定時間経過していなければ、会話が断続的に続いていると判断し、再度ステップS47を繰り返して会話がとぎれるのを待機する。

【0098】ステップS48では、鍵変更部6が、暗号化された新たなチャンネル暗号鍵及び暗号鍵IDを、チャットクライアントを介して他のユーザ端末に送信する。ステップS49では、当該ユーザ端末のチャットクライアントがチャンネルから退出したか否かを判断し、退出していれば処理を終了する。退出していなければ、再びステップS42に戻り、前記処理を繰り返す。

【0099】ステップS41で鍵変更属性がないと判断された場合、または、ステップS42で鍵変更属性の優先順位が第2位以下であると判断された場合、ステップS50に移行して新たなチャンネル暗号鍵の取得を行う。ステップS50では、鍵取得部4が、前回のチャンネル暗号鍵の変更から所定時間経過するのを待機し、所定時間が経過するとステップS51に移行する。本実施形態例においては、鍵取得部4は、ユーザ端末内の内部時計を参照することにより、前回のチャンネル暗号鍵の変更からの経過時間を監視する。

【0100】ステップS51では、鍵取得部4が新たなチャンネル暗号鍵を取得したか否かを判断し、まだ取得していなければ鍵取得部4はユーザ管理部3に対して優先順位の繰り上げを通知し、ステップS52に移行する。取得していれば後述するステップSに移行する。ステップS52では、前記通知を受けたユーザ管理部3が、鍵変更属性の優先順位が第2位以降のユーザの優先順位を順次繰り上げ、ユーザ情報の書き換えを行う。これにより、書き換え前は第2位以降であったユーザ全ての優先順位が変化する。

【0101】ステップS53では、優先順位の書き換えにより優先順位が第1位になったか否かを鍵変更部6により判断し、第1位であればステップS43に移行して前記チャンネル暗号鍵の変更を行う。優先順位が第2位以降であれば、前記ステップS50に移行し、新たなチャンネル暗号鍵の取得を行う。ステップS54では、他のユーザ端末から送信された新たなチャンネル暗号鍵を取得したので、鍵取得部4が、暗号化されたチャンネル暗号鍵を直前のチャンネル暗号鍵を用いて復号化し、新たなチャンネル暗号鍵を得る。

【0102】ステップS55では、取得部が、得られた

チャネル暗号鍵と暗号鍵IDとを対応付けて暗号鍵リストに格納する。ステップS56では、当該ユーザ端末のチャットクライアントがチャネルから退出したか否かを判断し、退出していれば処理を終了する。退出していなければ、再びステップS41に戻り、前記処理を繰り返す。

【0103】＜第2実施形態例＞チャットクライアント間で1対1の会話を行う場合は、会話の開始元の鍵取得部4が、相手先に対して自分の公開鍵を付加してセッション鍵要求を出す。要求を受けた相手先では、鍵生成部7がセッション鍵を生成し、要求元の公開鍵でセッション鍵を暗号化して要求元に送る。セッション鍵は、前記第1実施形態例と同様、会話の開始元や相手先の固有情報、時刻、クライアントに内蔵される秘密情報の組合せに対し、ハッシュ関数をかけて生成すると良い。

【0104】さらに、前記第1実施形態例と同様、新規セッション鍵は直前のセッション鍵を用いて暗号化して相手先に送ることが好ましい。また送信の際には、新規セッション鍵を相手先の公開鍵で暗号化して送信することが好ましいのも第1実施形態例と同様である。要求元の鍵取得部4は、ユーザの秘密鍵でセッション鍵を復号化し、記憶部2に格納する。以降、相互にセッション鍵によってメッセージを暗号化して会話を行う。

【0105】セッション鍵の変更のタイミングや条件は、前記第1実施形態例と同様である。すなわち、所定時間が経過したとき、所定会話数を超過したとき、所定会話量を超過したときなどにセッション鍵を変更する。また、セッション鍵の変更は、会話の開始元が行っても、また会話の相手先が行ってもよい。セッション鍵の変更を、前回メッセージを送信した方が行ったり、前回メッセージを受信した方が行ったりしてもよい。

【0106】なお、会話開始の要求を受けた鍵配布部5が、要求に付加されている公開鍵の正当性をチェックし、不当な場合は要求を受け付けないことはいうまでもない。公開鍵は、通常利用者端末に内蔵されている認証局の電子署名が施された公開鍵や、接続中のサーバの電子署名が施された公開鍵や、自らが電子署名した公開鍵を正当として認めることが考えられる。

【0107】＜第3実施形態例＞前記の第1実施形態例においては、セキュリティ強化装置1に設けたユーザ管理部3により鍵配布属性及び鍵変更属性を設けたが、他の方法も可能である。例えば、チャネルオペレータ属性などと同様に、鍵配布属性及び鍵変更属性をチャットシステム上のユーザ属性として設ける。各チャットクライアントは、ニックネームやチャネルオペレータ属性などと同様に、鍵配布属性及び鍵変更属性をユーザ情報の一部としてチャットサーバから取得し、ユーザDBに格納する。セキュリティ強化装置は、ユーザDB内のユーザ情報を参照し、前述の処理を行う。

【0108】＜第4実施形態例＞前記の第1実施形態例

においては、チャネル暗号鍵を変更するタイミングを鍵取得部4により監視しているが、他の形態も考えられる。例えば、鍵生成部7、鍵配布部5及び鍵変更部6は、チャネル暗号鍵と共にチャネル暗号鍵が次に変更される時刻を送信する。各ユーザ端末は、チャネル暗号鍵と共にチャネル暗号鍵の有効期限を持つことになる。各ユーザ端末の鍵取得部4は、チャネル暗号鍵の有効期限をチャネル暗号鍵の変更タイミングとする。チャネル暗号鍵と共にチャネル暗号鍵の有効期限を示す時刻を送信することにより、チャネル暗号鍵の変更を所定時間毎に行うことはもちろん、任意のタイミングで行うことが出来る。

【0109】もっとも、各ユーザ端末において内部時計にずれがある場合も考えられる。そこで、チャネル暗号鍵の有効期限を示す情報として、時刻に代えて相対時間及び起点時刻を用いることが考えられる。起点時刻としては、チャネル暗号鍵が生成された時刻を用い、相対時間としては、生成時刻を起点とした場合に次にチャネル鍵が変更されるまでの時間を用いる。

【0110】また前述のように、時間に基づくのではなく他の変化が生じた場合、例えばチャネル内ユーザが一人になった場合にチャネル暗号鍵の変更を行うこともあり得る。このような設定では、変化の頻度が少なすぎ、チャネル暗号鍵が長時間変更されない場合も考えられる。このような場合を防止する方法として、例えば次のような方法が挙げられる。

【0111】通常、鍵の生成に用いられるアルゴリズムは、鍵に有効期限を持たせている。そこで、鍵生成部7、鍵配布部5及び鍵変更部6により、チャネル暗号鍵と共にその有効期限を各ユーザ端末に送信する。鍵取得部4は、チャネル暗号鍵の有効期限まで所定の変化が生じなかった場合、有効期限をチャネル暗号鍵の変更タイミングとする。

【0112】

【発明の効果】チャットクライアント間でチャネル暗号鍵を分散管理し、クライアント間で公開鍵暗号を利用して鍵の配布を行い、チャネル暗号鍵を共有する。サーバに無関係に、クライアント間でチャネル暗号鍵を生成し、配布するので、サーバにメッセージ内容が漏洩することなく、チャネル内の会話のセキュリティを高めることが出来る。また、クライアント間で、メッセージの暗号化／復号化が行われるため、クライアント側に負荷が分散され、サーバの負荷を軽減することが出来る。

【図面の簡単な説明】

【図1】第1実施形態例に係るセキュリティ強化装置の機能ブロック図。

【図2】ユーザ情報の一例を示す説明図。

【図3】第1実施形態例に係るセキュリティ強化装置が行う主な処理の流れを示すフローチャート。

【図4】鍵取得処理の流れを示すフローチャート。

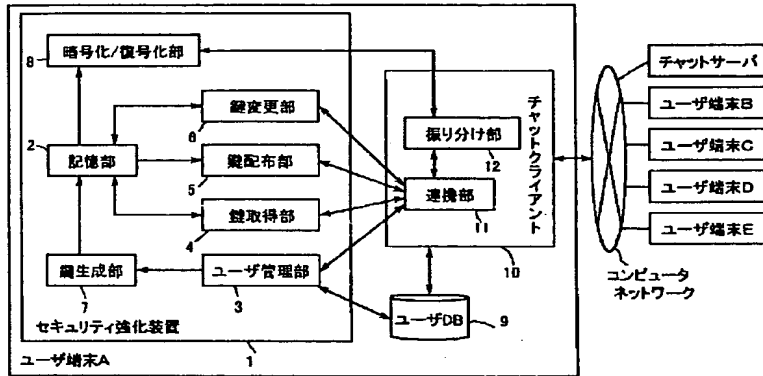


【図5】鍵配布処理の流れを示すフローチャート。

\* 【図7】鍵変更処理の流れを示すフローチャート。

【図6】要求検証処理の流れを示すフローチャート。 \*

【図1】



【図2】

ユーザ情報の概念説明図

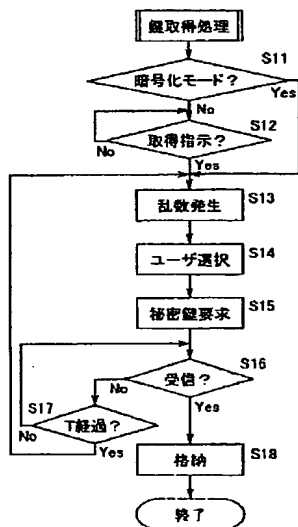
ニックネーム	Real Name	ユーザID	クライアント名	サーバ名	接続チャネル	アイドル時間 (sec)	Channel Operator	鍵配布 属性	鍵変更 属性	優先順位
taro	浦島 太郎	urushima	kame.ryugu.com	ryugu.com	#ryugu.#kame	90	1	1	1	1
hanako	富士 透花子	fujitsu	hana.fujitsu.com	fujitsu.com	#fujitsu.#ryugu	60	1	1	1	2
...	...	...	...	...	...	...	...	...	...	...

【図4】

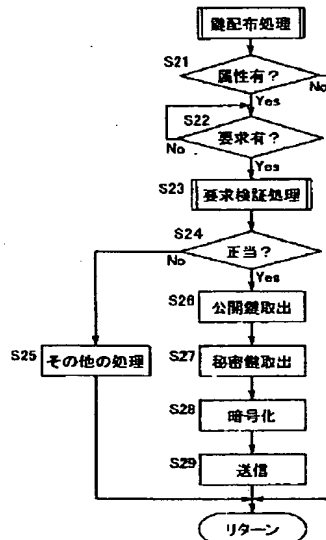
【図5】

【図6】

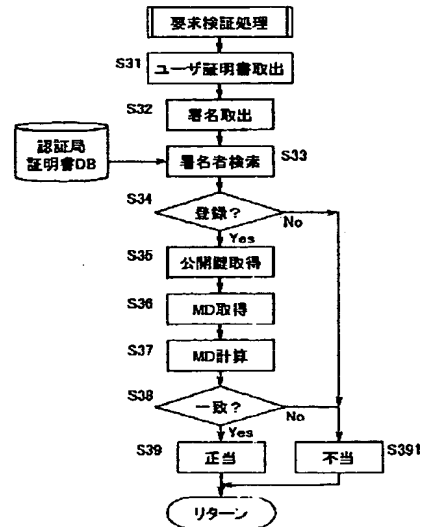
鍵取得処理の流れを示すフローチャート



鍵配布処理の流れを示すフローチャート

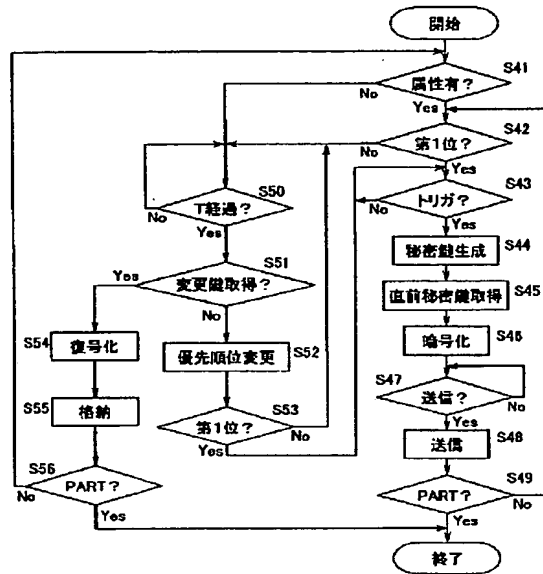


要求検証サブルーチン



【図7】

鍵変更処理の流れを示すフローチャート



フロントページの続き

F ターム(参考) 5B089 GA21 JA18 JB22 KA13 KA17  
 KB13 KC15 KC28 KC39 KC57  
 KE06 KH30  
 5J104 AA01 AA16 EA02 EA16 JA03  
 NA02 NA37 PA07